II. Remarks

Reconsideration and allowance of the subject application are respectfully requested.

Claims 1-54 are pending in the application. Claims 1, 3, 4, 6, 17, 29, 34, 46, and 54 are independent.

The undersigned and inventor Steve Davis would like to thank Examiners Arani and Hoffman for the cordial and productive interview of December 7, 2005. The Examiners' helpful comments and suggestions were instrumental in preparing this response.

Claims 1-58 were rejected as being unpatentable over Furukawa and Cornelius, for the reasons discussed on pages 2-11 of the Office Action. Applicant respectfully traverses all art rejections.

As discussed at the interview, Applicant's invention utilizes random data interleaved with a secret identifier (e.g., a PIN) in a truly random way. In the present invention, the random interleaving is known only to the sender and not to the receiver (i.e., random as to the whole world). As discussed at the interview, all of the cited art comprises *pseudo*-random data and processes whereby the random interleaving process is known to both the sender and the receiver so that the sent message can be decrypted (i.e., random only to third parties). As suggested by the Examiners during the interview, the claims have been amended to clarify the difference between the one-time truly random interleaving process according to the present invention from the *pseudo*-random interleaving process according to the cited art. Since the present amendments are clarifying only, it is respectfully suggested that no new issues have been presented which would require further consideration or search.

As also discussed during the interview, there are many ways that randomization can be used in security applications. First, random data can either be "real" where it is generated by a noise source or other actual random process in nature, or pseudo-randomization where the source of random data is a cryptographic function known to both the sender and the receiver. Second, random data can be used as a seed to initialize a function. In this case, the random data is simply used to provide a unique start to a session. Third, random information can be used to conceal information from third parties. This can be done either with a cryptographic function or true random data (such as a one-time pad). The subject invention is novel in its use of "true" random interleaving process by the sender, i.e., where the receiver does not have a key or code to decrypt the message. This random interleaving is entirely unknown to the receiver. In the disclosed embodiment, the receiver's server searches through the received sequence for the actual PIN data. Thus, the "random" interleaving is a one-time true random process, as opposed to the cited art in which the process must be known to both the sender and the receiver.

In view of the above, it is believed that this application is now in condition for allowance, and a Notice thereof is respectfully requested.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 625-3507. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicant
Richard P. Bauer
Registration No. 31,588

Patent Administrator
KATTEN MUCHIN ROSENMAN LLP
525 West Monroe Street
Chicago, Illinois 60661-3693
Facsimile: (312) 902-1061